**Daniele Berardi  
Maria Flavia Minotti  
  
TASK 01 MODELLO DESIGN DI RETE AZIENDALE DELLA COMPAGNIA THETA**

**INTRODUZIONE**

Di seguito si propone un modello (design) di rete per mettere in sicurezza le due **componenti critiche** dell’azienda:

1. **DMZ**: zona di rete in cui risiedono i servizi messi a disposizione del pubblico da parte della Theta.
2. **Rete interna**: composta da una Vlan per i dipendenti e una Vlan e-commerce che espone sulla rete interna un applicativo di e-commerce accessibile ai soli impiegati.

Inoltre, si include l’**analisi dei dispositivi di sicurezza** utili per aumentare la protezione della rete.

Immagine che contiene mappa, diagramma, testo

Descrizione generata automaticamente **STRUTTURA GENERALE DELLA RETE**

1. **ZONA DI RETE ESTERNA E COLLEGAMENTO AD INTERNET:**

* **Cloud:** simbolo della zona Wlan, rete esterna di internet.
* **Router provider:** dispositivo del provider del servizio di rete (Tim, Vodafone etc.) che funziona da router di transito tra la rete esterna di internet e la rete aziendale (core network)

1. **DMZ**

È una zona della rete Intranet, configurata come intermedia tra la rete esterna e le Vlan della rete locale, in cui la società Theta espone i servizi per l’accesso al pubblico. Essendo consentita la comunicazione in entrata e in uscita, si espongono i servizi e le Web application ad elevato rischio di attacchi informatici; pertanto, la DMZ è protetta da due firewall e da un IDS.

Per consentire agli utenti di sfruttare i servizi, la Theta utilizza i seguenti server. Come si vede dallo schema, all’interno della zona è presente:

* Il **Web server**: che offre i servizi della società al pubblico, utilizzando il protocollo HTTP.
* **Server FTP:** che permette di accettare connessioni in entrata e di comunicare con un client attraverso il protocollo FTP.
* **Server Mail:** consente l’invio, tramite protocollo SMTP, e la ricezione, attraverso protocolli IMAPS, dei messaggi di posta elettronica.
* **Switch:** device che consente la connessione tra i server all’interno della stessa rete DMZ. Si sono previsti un numero superiore di switch per supportare l’implementazione del sistema di backup.
* **Server di Backup:** sono presenti copie di ciascun server delle web application in modo da garantire l’archiviazione e il ripristino dei dati in caso di malfunzionamenti o attacchi informatici.Nel grafico si sono spente le connessioni dei server di backup per mostrare che sono attivabili per ripristinare i servizi precedentemente forniti dai server compromessi da attacchi o malfunzionamenti.  
  E’ in ogni caso previsto un cavo di collegamento sata tra server principale e backup per riuscire a effettuare i backup previsti ogni 24h.
* **WAF:** è un tipo di firewall che protegge le applicazioni web offerte dalla Theta da minacce provenienti dall’esterno. Il vantaggio è che il WAF analizza il traffico in entrata e in uscita per identificare e bloccare le attività sospette o pericolose.
* **IDS**: è il Sistema di Rilevamento delle Intrusioni che avvisa con notifica gli amministratori di sistema, circa l’esistenza di una possibile minaccia nella rete. In particolare, monitorando il traffico di rete, i log di sistema e altri eventi, identifica firme o modelli noti di attacchi informatici, comportamenti anomali o violazioni delle policy di sicurezza
* **Firewall stateful:** è un tipo di firewall che tiene conto non solo del traffico di rete ma anche dello stato delle connessioni di rete. Il vantaggio di un simile dispositivo di sicurezza sta nella sua capacità di monitorare le connessioni in real time e ricordare quelle precedenti. In particolare, riconosce le connessioni già stabilite e consente automaticamente il traffico associato a quelle connessioni. In tal modo le connessioni che in passato sono state considerate dannose vengono automaticamente bloccate.

1. **RETE PRIVATA (Nel grafico, area in verde)**

* **Vlan e-commerce**: zona della rete interna alla quale possono accedere esclusivamente i dipendenti della Theta. Si distinguono le due reti in modo tale da inserire un dispositivo di sicurezza che rilevi un eventuale comportamento anomalo dei dipendenti. Al suo interno si trovano i seguenti server:
* **Server Nas**: che offre uno spazio di archiviazione di file digitali e permette il back up dell’e-commerce, cioè di avere copie complete dei file archiviati per un possibile ripristino in caso di perdita dei dati (per via di attacco informatico o guasto tecnico).
* **Server HTTP e-commerce**: che offre i servizi dell’e-commerce ai dipendenti, utilizzando il protocollo HTTP.
* **Server DHCP**-**DNS:** utilizzato sia per attribuire dinamicamente l’indirizzo IP e altri parametri a ciascun dispositivo dei dipendenti in modo che possano comunicare con tutta la rete interna, sia per tradurre l’indirizzo ip del server in url (nome di dominio dell’e-commerce) e viceversa.
* **Switch:** device che consente la connessione tra i tre server all’interno della stessa rete Vlan e-commerce.
* **IDS:** è il Sistema di Rilevamento delle Intrusioni che avvisa con notifica gli amministratori di sistema, circa l’esistenza di una possibile minaccia nella rete. In particolare, monitorando il traffico di rete, i log di sistema e altri eventi, identifica firme o modelli noti di attacchi informatici, comportamenti anomali o violazioni delle policy di sicurezza.
* **WAF:** è un tipo di firewall che protegge le applicazioni web offerte dalla Theta da minacce provenienti dall’esterno e da eventuali attacchi voluti o meno provenienti dalla VLAN dipendenti. Il vantaggio è che il WAF analizza il traffico in entrata e in uscita per identificare e bloccare le attività sospette o pericolose.
* **Vlan amministratore:** zona della rete dell’amministratore di rete che si occupa di gestire, monitorare, provvedere alla manutenzione e alla sicurezza dell’intera Intranet aziendale.
* **Firewall stateless:** misura di sicurezza che tutela la sottorete dell’amministratore.
* **Vlan dipendenti:** zona della rete interna che ospita i device dei dipendenti.
* Le tre zone della rete interna sono collegate tramite **router3** e l’accesso alle tre è regolata dalla presenza di un **Next Generation Firewall (NGFW):** è un componente di sicurezza automatizzata tra i più avanzati perché racchiude in se una serie di funzionalità aggiuntive rispetto ai firewall tradizionali: controllo approfondito dei pacchetti e del traffico tra device dai livelli da 2 a 7 del modello ISO/OSI, capacità di regolazione dell’ accesso alle zone protette con l’identificazione degli utenti autorizzati, e la capacità di prevenire e bloccare un’ampia varietà di attacchi informatici (spesso sono integrati i sistemi di sicurezza IPS e IDS). Nel design di rete proposto si è deciso di rafforzare la funzionalità di identificazione degli utenti prevedendo un **Nac,** ovvero un sistema di sicurezza utilizzato per controllare e limitare l'accesso a una rete, aiutando in tal modo a proteggere gli endpoint creando policy e mettendo in quarantena i sistemi non conformi.

Tramite NGFW e NAC l’amministratore di sistema può impedire completamente l’accesso dalla rete esterna alla Vlan e-commerce e alla Vlan Amministratore e di filtrare la comunicazione tra Vlan dipendenti e la rete esterna**.** Ciò si traduce nel fatto che, a seconda delle policy adottate, i dipendenti potranno o meno accedere alla rete internet.

1. **ZONA DI “TRAPPOLA” O “HONEY NET AD ALTA INTERAZIONE”**

È una parte non protetta della rete aziendale composta da device che sono volutamente esposti ad attacchi informatici per un duplice scopo:

* 1) indurre eventuali malintenzionati ad attaccare la zona di trappola piuttosto che le altre zone di rete.
* 2) raccogliere informazioni circa l’attacco e l’attaccante: gli honey pot inducono gli hacker a indugiare il più a lungo possibile al loro interno, svelando i metodi, gli strumenti, gli obiettivi e le vulnerabilità interne utilizzate per l’attacco.

Per realizzare il duplice scopo e indurre in trappola i malintenzionati, si è proceduto a configurare l’Honey net subito dopo la DMZ e prima del Firewall Nac. Infatti, così un eventuale aggressore, dopo aver aggirato i firewall della DMZ, crederebbe di aver raggiunto una vera rete interna.

**ANALISI DISPOSITIVI DI SICUREZZA PER LA PROTEZIONE DELLA RETE**

Dopo l’analisi della composizione della rete, si riporta un’analisi dei sistemi di sicurezza ritenuti necessari e sufficienti per la tutela della rete stessa.

Il **WAF** è la prima barriera difensiva posta a salvaguardia della DMZ perché è il firewall progettato appositamente per le web application in quanto in grado di difendere da un'ampia gamma di attacchi a livello di applicazione che sono invisibili ad altri tipi di firewall, ed è seguito da un **IDS** per inviare allarme agli amministratori di sistema in caso di un eventuale compromissione nonostante la presenza del WAF.

Il **Firewall Stateful** è la barriera di chiusura della DMZ e la prima barriera difensiva della rete privata aziendale in quanto in grado di effettuare un controllo avanzato del traffico proveniente dalla zona di rete non sicura e da rete Internet. In particolare, tale firewall è stato scelto per la capacità di semplificare la comunicazione, garantendo al contempo la necessaria protezione. Infatti, in tal modo lo Stateful consente solitamente le connessioni già stabilite precedentemente e bloccherà quelle che invece sono potenzialmente dannose. L'autore di un attacco dovrebbe compromettere entrambi i firewall per avere accesso alla LAN privata della Theta. Si sarebbe potuto inserire anche un Firewall più avanzato per la sicurezza ma è stato ritenuto non necessario in vista della funzione di trappola della Honey Net e della successiva barriera rafforzata rappresentata dall’NGFW.

Le tre VLan, dipendenti, E-commerce e Amministratore sono protette da un **Next Generation Firewall e da un NAC** in quanto, intervenendo sulle impostazioni nel policy set, si permette un eventuale connessione limitata con la rete esterna della Vlan dipendenti (come anche un completo isolamento della stessa) e si impedisce completamento l’accesso alla Vlan e-commerce che è ad uso e consumo esclusivo dei dipendenti. Come già accennato in precedenza, inoltre, questo tipo di Firewall è stato scelto per la capacità di tutelare la rete privata da attacchi informatici sofisticati come quelli che sfruttano i ransomware o gli zero day. L’amministratore di rete ha il privilegio di bypassare e settare i due strumenti di sicurezza per intervenire sul resto della rete. Per quanto attiene alla sicurezza interna alla stessa rete privata (area in verde), si è previsto un **Firewall Stateless** posizionato sulla Vlan dipendenti per impedire l’accesso alla Vlan Amministratore. Qualora il/i dipendente/i dovesse/ro aggirare il firewall si sono previsti **due IDS** sulle altre due sottoreti della rete privata per avvertire con notifica di allarme l’amministratore.   
L’ application server è tutelato ulteriormente da un WAF e un IDS come avveniva per il Web Server. Questi due strumenti tutelano quindi l’Application Server non solo da eventuali attacchi esterni ma anche da comportamenti sospetti o veri e propri attacchi informatici che dovessero giungere dai clients dei dipendenti.